STATE OF ALABAMA

Information Technology Policy

Policy 620-03: Authentication

OBJECTIVE:
Define the minimum requirements for authenticated access to State information system resources.

SCOPE:
This policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

RESPONSIBILITIES:
Every user shall be assigned a unique user identification and authentication mechanism (e.g., user ID and password) so all activities on the network are traceable to a specific user.

At a minimum, users shall uniquely identify themselves to the system or network resource and authenticate that identification with at least one authentication factor.

Authentication factors include (but are not limited to) passwords, pass-phrases, biometric signatures (e.g., fingerprint, retina scan, etc), keys, cards, etc., and may be required in any combination (i.e., multi-factor authentication). Detailed authentication requirements shall be documented in applicable standards and procedures.

Authentication factors must never be shared, cached, stored in any readable form, or kept in locations where unauthorized persons might discover them.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.

By Authority of:

Chief Information Officer

3/9/06

Date

Policy History

Version	Release Date	Comments
Original	3/9/2006	